

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344207

(43)Date of publication of application : 14.12.2001

(51)Int.Cl.

G06F 15/00

G06F 15/16

G06F 15/163

H04L 9/32

H04L 12/22

(21)Application number : 2000-162507

(71)Applicant : NEC CORP

(22)Date of filing : 31.05.2000

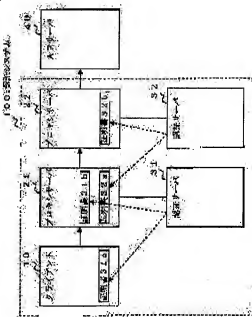
(72)Inventor : YOKOI HIDEHIKO

## (54) CERTIFICATION SYSTEM AND ITS METHOD

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To solve such a conventional problem that each certification server should be provided with a specific function for transferring a registered user's certificate between certification servers.

**SOLUTION:** In the certification system 100 constituted of a client 10 connected to a communication line, plural proxy servers 21, 22 interposed between the client 10 and a server 40 and plural certification servers 31, 32 formed correspondingly to respective proxy servers 21, 22, the servers 31, 32 respectively execute certification on the basis of certificates distributed to the corresponding proxy servers 21, 22 and the connection sources of the servers 21, 22. The proxy server 21 repeating the client 10 and the proxy server 22 transfers a certificate 31a owned by the client 10 to the proxy server 22. Thereby it is unnecessary to transfer the registered user's certificate between the certification servers 31, 32.



## LEGAL STATUS

[Date of request for examination] 13.04.2001

[Date of sending the examiner's decision of rejection] 07.12.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許公開番号

特開2001-344207

(P2001-344207A)

(43) 公開日 平成13年12月14日 (2001.12.14)

(51) Int.Cl.<sup>1</sup>

識別記号

F I

テーマコード (参考)

G 0 6 F 15/00

3 3 0

G 0 6 F 15/00

3 3 0 A 5 B 0 4 5

15/16

6 2 0

15/16

6 2 0 B 5 B 0 8 5

15/163

6 5 0

15/163

6 5 0 X 5 J 1 0 4

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 D 5 K 0 3 0

12/22

11/26

審査請求 有 請求項の数 6 O L (全 12 頁)

(21) 出願番号

特願2000-162507(P2000-162507)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(22) 出願日

平成12年5月31日 (2000.5.31)

(72) 発明者 横井 英彦

東京都港区芝五丁目7番1号 日本電気株式会社社内

(74) 代理人 100086759

弁理士 渡辺 喜平

Fターム (参考) 5B045 BB19 BB28 BB47 BB48 GG09

5B085 AE23 BC07

5J104 AA07 BA02 KA01 MA03 PA07

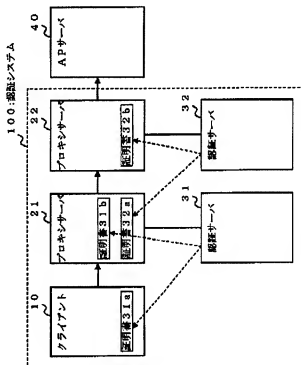
5K030 GA15 HC01

(54) 【発明の名称】 認証システムおよび認証方法

(57) 【要約】

【課題】 登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能が各認証サーバに備わっていなければならなかった。

【解決手段】 通信回線に接続されたクライアント10、クライアント10とサーバ40との間に介在する複数のプロキシサーバ21、22、それぞれのプロキシサーバに対応して設けられた複数の認証サーバ31、32とにより構成される認証システム100において、認証サーバ31、32は、対応するプロキシサーバ21、22とこのプロキシサーバ21、22の接続元とに配布した証明書に基づいて認証を行う。そして、クライアント10とプロキシサーバ22とを中継するプロキシサーバ21が、クライアント10が保有する証明書31aをプロキシサーバ22に受け渡す。その結果、登録されたユーザの証明書を認証サーバ間で受け渡す必要がなくなる。



#### 【特許請求の範囲】

【請求項1】 通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに、対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとを具備する認証システムであって、上記認証サーバは、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、

上記プロキシサーバは、接続先から上記クライアントに証明書を要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、

上記クライアントは、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信することを特徴とする認証システム。

【請求項2】 上記請求項1に記載の認証システムにおいて、

上記サーバに最も近いプロキシサーバは、接続元との間の認証が完了したとき、この接続元へ上記証明書要求を送信することを特徴とする認証システム。

【請求項3】 上記請求項1あるいは請求項2のいずれかに記載の認証システムにおいて、

上記プロキシサーバは、上記クライアントに配布された上記証明書とあわせて、自らに配布された上記証明書を接続先へ送信することを特徴とする認証システム。

【請求項4】 上記請求項1～請求項3のいずれかに記載の認証システムにおいて、

上記プロキシサーバは、自らに配布された上記証明書を上記証明書要求に添付して接続元へ送信し、上記クライアントは、上記プロキシサーバに配布された上記証明書を確認して、配布された上記証明書を接続先へ送信することを特徴とする認証システム。

【請求項5】 上記請求項1～請求項4のいずれかに記載の認証システムにおいて、

上記クライアントは、上記サーバへの接続を要求してから所定時間内に上記証明書要求を入力することができないうとき、自らに配布された証明書の引き渡しを中止することを特徴とする認証システム。

【請求項6】 通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに、対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとにより構成される認証方法であつて

上記認証サーバにて、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、

上記プロキシサーバにて、接続先から上記クライアントに証明書を要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、

上記クライアントにて、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信することで認証を行うことを特徴とする認証方法。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、認証システムおよび認証方法に関し、特に、通信回線に接続されたクライアント、クライアントとサーバとの間に介在する複数のプロキシサーバおよびこれらのプロキシサーバに対応して設けられた複数の認証サーバとにより構成される認証システムおよび認証方法に関する。

##### 【0002】

【従来の技術】従来より、この種の認証システムは、通信回線に接続されたクライアント、クライアントとサーバとの間に介在する複数のプロキシサーバおよび複数の認証サーバとにより構成されている。複数の認証サーバは、それぞれのプロキシサーバに対応して設けられている。そして、予め、すべてのプロキシサーバに属する認証サーバはクライアントを使用するユーザを登録するとともに、クライアントへ証明書を配布する。その上で、配布した証明書に基づいて、認証サーバが対応するプロキシサーバとこの接続元との間の認証をクライアント側から順番に行う。その結果、各プロキシサーバにてクライアントを使用するユーザを認証することが可能となる。しかし、すべての認証サーバからクライアントに証明書を配布しなければならないため、ユーザの管理だけで多大な作業が必要になる。

【0003】この作業を軽減させるため、クライアントに最も近い認証サーバにだけユーザを登録させる構成とした認証システムも知られている（特開平11-328117号公報）。この認証システムは、登録されたユーザの証明書を認証サーバ間で受け渡していくことで、プロキシサーバとこの接続元との間の認証をクライアント側から順番に行う。これは、クライアントと各プロキシサーバとの認証が行われる際に、各認証サーバでユーザの証明書が必要となるためである。すると、認証サーバすべてにクライアントのユーザ情報を登録しなくても、各プロキシサーバにてクライアントを使用するユーザを認証することが可能となる。

##### 【0004】

【発明が解決しようとする課題】しかしながら、上述した従来の認証システムにおいては、登録されたユーザの

証明書を送信サーバ間で受け渡していくという特別の機能が各認証サーバに備わっていなければならない。

【0005】本発明は、上述の課題にかながみてなされたもので、各認証サーバに特別の機能が備わっていても、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能な認証システムおよび認証方法の提供を目的とする。

【0006】

【課題を解決するための手段】 上述の目的を達成するため、請求項1にかかる発明は、通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに対応する上記プロキシサーバの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとを具備する認証システムであって、上記認証サーバは、対応する上記プロキシサーバとこのプロキシサーバの接続元とに配布した証明書に基づいて認証を行い、上記プロキシサーバは、接続先から上記クライアントに証明書を送信する証明書を要求が入力されたときこの証明書を要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続元へ送信し、上記クライアントは、接続先からの上記証明書を要求に応じて配布された上記証明書を接続元へ送信する構成としてある。

【0007】すなわち、クライアント、複数のプロキシサーバ、複数の認証サーバは、通信回線を介して双方向通信可能に接続されている。複数のプロキシサーバは、クライアントとサーバとの間に介在して、クライアントとサーバとを接続させることが可能である。複数の認証サーバは、それぞれのプロキシサーバに対応して設けられており、対応するプロキシサーバとこのプロキシサーバの接続元との間の認証を行う。なお、クライアントに最も近いプロキシサーバの接続元はクライアントであり、それ以外のプロキシサーバの接続元は別のプロキシサーバとなる。

【0008】認証サーバは、予め、対応するプロキシサーバとこの接続元に証明書を配布する。その上で、配布した証明書に基づいて、複数の認証サーバが対応するプロキシサーバとこの接続元との間の認証をクライアント側から順番に行う。その際、この認証サーバから対応するプロキシサーバとこの接続元とに配布された証明書を確信することで、プロキシサーバとこの接続元との間の認証を行う。

【0009】クライアントとサーバとを中継するプロキシサーバは、接続先からクライアントに証明書を送信する証明書を要求が入力されたとき、この証明書を要求を接続元へ送信する。接続元が別のプロキシサーバであれば、接続先のプロキシサーバと同様、入力された証明書を要求を接続元へ送信する。そして、接続元がクライアントと

なったとき、クライアントはこの証明書要求に応じて、自らに配布されるとともに、認証済みの証明書を接続先のプロキシサーバへ送信する。すると、クライアントに最も近いプロキシサーバは、この認証済みの証明書を受け取り接続先へ送信する。接続先がプロキシサーバであれば、接続元のプロキシサーバと同様、この認証済みの証明書を入手して接続先へ送信する。

【0010】すなわち、クライアントに配布された証明書は、認証されるとともに、クライアントとサーバとを中継する複数のプロキシサーバに受け渡されることとなる。すると、各プロキシサーバにて、クライアントが保有する認証済みの証明書を確信することが可能となる。したがって、すべての認証サーバにクライアントを使用するユーザを登録する必要がなく、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能となる。その際、登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能は不要である。

【0011】ここで、クライアントに証明書を要求する証明書要求の出力元は様々可能であり、その具体的な構成の一例として、請求項2にかかる発明は、請求項1に記載の認証システムにおいて、上記サーバに最も近いプロキシサーバは、接続元との間の認証が完了したとき、この接続元へ上記証明書を要求を送信する構成としてある。すなわち、サーバに最も近いプロキシサーバとこの接続元のプロキシサーバとの間の認証が完了したとき、サーバに最も近いプロキシサーバが証明書要求を接続元へ送信する。すると、サーバに最も近いプロキシサーバとクライアントとを中継するプロキシサーバが、この証明書要求をクライアントまで送信する。したがって、サーバに最も近いプロキシサーバにて、クライアントを使用するユーザの認証を行うことが可能となる。もちろん、証明書要求の出力元がサーバに最も近いプロキシサーバである構成は一例に過ぎず、他のプロキシサーバが出力元であってもよいし、外部のサーバが出力元であっても、様々可能である。

【0012】認証サーバに配布する証明書は、クライアントやプロキシサーバを識別する情報であればよい。また、プロキシサーバに受け渡す証明書はクライアントに配布された証明書に限定されず、その構成の一例として、請求項3にかかる発明は、請求項1あるいは請求項2のいずれかに記載の認証システムにおいて、上記プロキシサーバは、上記クライアントに配布された上記証明書とあわせて、自らに配布された上記証明書を接続先へ送信する構成としてある。すなわち、プロキシサーバは、クライアントが保有する認証済みの証明書とあわせて他のプロキシサーバが保有する認証済みの証明書を確信することができる。したがって、より確実に認証を行うことができる。

【0013】また、各プロキシサーバに配布された証明

書をさらに活用する構成の一例として、請求項4にかかる発明は、請求項1～請求項3のいずれかに記載の認証システムにおいて、上記プロキシサーバは、自らに配布された上記証明書を上記証明書要求に添付して接続元へ送信し、上記クライアントは、上記プロキシサーバに配布された上記証明書を確認して、配布された上記証明書を接続先へ送信する構成としてある。すなわち、クライアントは、プロキシサーバが保有する認証済みの証明書を受け取る。そして、受け取った証明書を確認したうえで、自らが保有する証明書をプロキシサーバに引き渡す。したがって、より確実に認証を行うことができる。

【0014】ところで、認証システムを構成するクライアント、複数のプロキシサーバ、認証サーバは通信回線により接続されているため、通信回線等の状態によっては認証するのに時間がかかりすぎることがある。そこで、請求項5にかかる発明は、請求項1～請求項4のいずれかに記載の認証システムにおいて、上記クライアントは、上記サーバへの接続を要求してから所定時間内に上記証明書要求を入手することができないとき、自らに配布された証明書の引き渡しを中止する構成としてある。すなわち、クライアントは、接続先のプロキシサーバから証明書要求が所定時間内に送信されない場合、自らが保有する証明書の引き渡しを中止する。したがって、通信の仕様が良好でない等の場合にサーバへの接続処理が中止されるため、本システムの利用価値をより高めることができる。

【0015】上述したように、クライアント、プロキシサーバ、認証サーバとからなるシステムにおいては、所定のプログラムが実行される。このプログラムは上述の手段に対応した所定の制御手順に従って処理を進めていく上で、その根拠にはその手順に発明が存在するということが当然である。

【0016】そこで、請求項6にかかる発明は、通信回線に接続されたクライアントと、この通信回線に接続されてこのクライアントとサーバとの間に介在する複数のプロキシサーバと、上記通信回線に接続されてそれぞれの上記プロキシサーバに対応して設けられるとともに対応する上記プロキシサーバへの接続元との間の認証を上記クライアント側から順番に行う複数の認証サーバとにより構成される認証方法であって、上記認証サーバにて、対応する上記プロキシサーバとこのプロキシサーバへの接続元とに配布した証明書に基づいて認証を行い、上記プロキシサーバにて、接続先から上記クライアントに証明書要求する証明書要求が入力されたときこの証明書要求を接続元へ送信するとともに、接続元から送信された上記クライアントに配布された上記証明書を接続先へ送信し、上記クライアントは、接続先からの上記証明書要求に応じて配布された上記証明書を接続先へ送信することで認証を行う構成としてある。すなわち、必ずしも

であり、基本的には同様の作用となる。また、請求項2～請求項5に記載されたシステム構成を当該方法に対応させることも可能であることは言うまでもない。

【0017】

【発明の実施の形態】以下、図面にもとづいて本発明の実施形態を説明する。図1は、本発明の一実施形態にかかる認証システムを概略図により示している。図1において、認証システム100は、双方向通信可能な通信回線に接続されたクライアント10、プロキシサーバ21、22、認証サーバ31、32とから構成されている。ユーザが、クライアント10からAPサーバ40へ接続を要求すると、所定の認証が完了した後、プロキシサーバ21、22を介してクライアント10とAPサーバ40との接続が確立するようにになっている。

【0018】クライアント10は、通信回線にアクセス可能な通信インタフェースを備え、通信回線に接続可能なコンピュータであればよい。そこで、クライアント10は、例えば各家庭で汎用的に用いられるパーソナルコンピュータであってもよいし、持ち運びの可能な携帯端末であってもよい。また、通信回線には所定のパーソナルコンピュータをローカルサーバにするなどしてLAN (Local Area Network) を接続することも可能である。すなわち、クライアント10の代わりにLANを接続し、このLAN内の複数のパーソナルコンピュータから通信回線にアクセスする構成としてもよい。

【0019】本実施形態のクライアント10は、所定のOSプログラムやアプリケーションプログラムを記憶するハードディスクを備えている。そして、CPU、ROM、RAM等によってこれらのOSプログラムやアプリケーションプログラムを実行する。また、ディスプレイ、キーボード、マウス等も備えており、OSプログラムの制御によりこれらを駆動している。

【0020】プロキシサーバ21、22は、クライアント10とAPサーバ40との間に介在して、クライアントとサーバとを接続させることが可能である。そのため、プロキシサーバ21、22は、通信回線にアクセス可能な通信インタフェースや、所定のプログラムを記憶するハードディスク等を備えたハードウェア構成となっている。そして、CPU、ROM、RAM等によりハードディスクに記憶されているプログラムを実行する。

【0021】認証サーバ31、32は、それぞれのプロキシサーバ21、22に対応して設けられており、対応するプロキシサーバ21、22とこのプロキシサーバ21、22の接続元との間の認証を行う。ここで、プロキシサーバ21の接続元はクライアント10であり、認証サーバ31がクライアント10とプロキシサーバ21との間の認証を行う。また、プロキシサーバ22の接続元はプロキシサーバ21であり、認証サーバ32がプロキシサーバ21とプロキシサーバ22との間の認証を行

う。なお、認証サーバ31、32のハードウェアの構成は、プロキシサーバ21、22と概略同様となっている。

【0022】認証サーバ31、32は、予め、対応するプロキシサーバ21、22との接続元になるクライアント10あるいはプロキシサーバ21とのユーザ登録を受け付ける。そして、クライアント10あるいはプロキシサーバ21、22に証明書を配布する。

【0023】本実施形態の場合、クライアント10からAPサーバ40へと接続を要求するユーザのユーザ情報は、クライアント10に最も近いプロキシサーバ21の属する認証サーバ31に登録される。認証サーバ31からは、ユーザの証明書31aがクライアント10に配布される。また、プロキシサーバ21としてのユーザ情報は、プロキシサーバ21の属する認証サーバ31と、次に中継されるプロキシサーバ22の属する認証サーバ32に登録される。認証サーバ31からは証明書31bが配布され、認証サーバ32から証明書32aが配布される。プロキシサーバ22としてのユーザ情報は認証サーバ32に登録され、認証サーバ32から証明書32bが配布される。

【0024】その上で、配布した証明書31a、31b、32a、32bに基づいて、認証サーバ31、32が対応するプロキシサーバ21、22との接続元との間の認証をクライアント側から順次に行う。ユーザがクライアント10からAPサーバ40へ接続要求を行うと、まず、認証サーバ31が証明書31aと証明書31bとを入手して認証を行う。この認証が成功すれば、プロキシサーバ21からプロキシサーバ22へ接続され、認証サーバ32が証明書32aと証明書32bとを入手して認証を行う。この認証が成功すると、所定の手順により、APサーバ40に最も近いプロキシサーバ22が保有する証明書32bと、クライアント10が保有する証明書31aとを、プロキシサーバ21を介して交換する。

【0025】ここで、クライアント10とプロキシサーバ21との間は、証明書31aと証明書31bとにより認証された状態である。また、プロキシサーバ21とプロキシサーバ22の間も、証明書32aと証明書32bとにより認証された状態である。すなわち、クライアント10とプロキシサーバ22の間は、プロキシサーバ21を介して認証済みの状態となっている。すると、交換された証明書32b、証明書31aは互いに信頼できる証明書である。そこで、プロキシサーバ22は、クライアント10を使用するユーザの証明書31aに基づいてAPサーバ40に接続を要求すると、クライアント10とAPサーバ40との接続も確立させることが可能となる。

【0026】したがって、ユーザ登録をクライアント10に最も近いプロキシサーバ21に対応する認証サーバ

31でのみ行うことで、各プロキシサーバにてユーザの認証を行うことが可能となる。その際、認証サーバ間でユーザの証明書を受け渡す必要がない。なお、クライアント10とプロキシサーバ22との間が認証済みの状態となったときに、クライアント10が保有する証明書31aだけをプロキシサーバ21を介してプロキシサーバ22に受け渡すだけでもよい。この場合でも、証明書31aは信頼できる証明書であるため、この証明書31aを用いて各プロキシサーバにてユーザの認証を行うことが可能である。

【0027】次に、本認証システム100におけるクライアント10、プロキシサーバ21、22にて実行される処理をフローチャートに沿って説明する。なお、本フローでは、プロキシサーバ21が保有する証明書31b、32aもクライアント10あるいはプロキシサーバ22に受け渡すことでより確実に認証を行う構成としている。図2、図3、図4は、それぞれクライアント10、プロキシサーバ21、プロキシサーバ22にて実行される処理の概略を示すフローチャートである。

【0028】まず、ユーザがクライアント10からAPサーバ40へ接続要求を行うと（図2のステップS100）、プロキシサーバ21はクライアント10からAPサーバ40への接続要求を受信する（図3のステップS200）。そして、プロキシサーバ21は、接続してきたユーザの認証を認証サーバ31へ要求する（ステップS205）。認証サーバ31から認証結果を受信すると（ステップS210）、ユーザの認証が成功かどうかを判断する（ステップS215）。認証が失敗であれば、ユーザからAPサーバ40への接続要求を拒否するとともに、接続要求拒否をクライアント10に通知し（ステップS220）、本フローを終了する。この場合、クライアント10では図示しないフローにて図2のフローを終了する。認証が成功であれば、接続先のプロキシサーバ22へAPサーバ40への接続要求を行う（ステップS225）。

【0029】プロキシサーバ22は、プロキシサーバ21からAPサーバ40への接続要求を受信すると（図4のステップS300）、接続してきたプロキシサーバ21の認証を認証サーバ32へ要求する（ステップS305）。認証サーバ32からその認証結果を受信すると（ステップS310）、プロキシサーバ21の認証が成功かどうかを判断する（ステップS315）。認証が失敗であれば、プロキシサーバ21からAPサーバ40への接続要求を拒否するとともに、接続要求拒否をプロキシサーバ21に通知し（ステップS320）、図4のフローを終了する。この場合、プロキシサーバ21では図示しないフローで接続要求拒否をクライアント10に通知し、図3のフローを終了する。認証が成功であれば、プロキシサーバ22は、接続元のプロキシサーバ21に

の証明書要求を送信する(ステップS325)。その際、自らが保有する認証済みの証明書32bを添付している。

【0030】すると、プロキシサーバ21は、プロキシサーバ22から、APサーバ40へ接続要求を行っているユーザの証明書要求を受信する(図3のステップS230)。そして、認証サーバ32で認証済みの証明書32bが添付されていることを確認する(ステップS235)。その上で、プロキシサーバ21はクライアント10に対して、APサーバ40へ接続要求を行っているユーザの証明書要求を送信する(ステップS240)。その際、証明書32bとあわせて、プロキシサーバ21が保有する認証済みの証明書31bをさらに添付している。

【0031】クライアント10では、プロキシサーバ21から、所定時間内にAPサーバ40へ接続要求を行っているユーザの証明書要求を受信したかどうかを判断する(図2のステップS105)。プロキシサーバ21から接続要求拒否が通知されるか、所定時間内にユーザの証明書要求を受信しなかった場合は、APサーバ40への接続要求を取り消す。したがって、通信の状態が良好でない等の場合に、APサーバ40への接続要求を必要以上に長時間行うことがない。

【0032】ユーザの証明書要求を受信した場合(ステップS110)、プロキシサーバ21に配布された証明書31bが添付されているとともに、認証サーバ31で認証済みであることを確認する(ステップS115)。また、証明書要求元であるAPサーバ40に最も近いプロキシサーバ22に配布された証明書32bが添付されているとともに、認証サーバ32で認証済みであることを確認する(ステップS120)。そこで、クライアント10は、プロキシサーバ21に対して、APサーバ40へ接続要求を行っているユーザの証明書31aを送信し(ステップS125)、図2のフローを終了する。

【0033】プロキシサーバ21では、クライアント10から、APサーバ40へ接続要求を行っているユーザの証明書31aを受信する(図3のステップS245)。そして、証明書31aが認証サーバ31で認証済みであることを確認する(ステップS250)。その上で、プロキシサーバ22に対して、APサーバ40へ接続要求を行っているユーザの証明書31aを送信し(ステップS255)、図3のフローを終了する。その際、プロキシサーバ21に配布された認証済みの証明書32aをさらに添付している。

【0034】プロキシサーバ22では、プロキシサーバ21から、APサーバ40へ接続要求を行っているユーザの証明書31aを受信する(図4のステップS330)。そして、認証サーバ32で認証済みの証明書32aが添付されていることを確認する(ステップS335)。また、APサーバ40へ接続要求を行って

いるユーザの証明書31aも認証済みであることを確認する(ステップS340)。その結果、プロキシサーバ22とユーザとが相互に認証できたこととなり、プロキシサーバ22はAPサーバ40へ接続要求を送信する(ステップS345)。すると、プロキシサーバ21、22を介してクライアント10とAPサーバ40との接続を確立させることが可能である。

【0035】このように、本認証システム100では、配布された証明書に基づいて、認証サーバにて対応するプロキシサーバとこの接続元との間の認証がクライアント側から順番に行われる。そして、クライアント10に配布された証明書31aがプロキシサーバ21を介してAPサーバ40に最も近いプロキシサーバ22に受け渡される。したがって、すべての認証サーバにクライアントを使用するユーザを登録する必要がなく、各プロキシサーバにてユーザを認証することが可能となる。その際、登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能は不要である。

【0036】また、クライアントは、各プロキシサーバが保有する認証済みの証明書を受け取って確認したうえで、自らが保有する認証済みの証明書を確認し、それに引き渡す。さらに、クライアントとサーバに最も近いプロキシサーバとを中継するプロキシサーバが保有する認証済みの証明書も、クライアントとサーバに最も近いプロキシサーバに受け渡され、確認される。したがって、より確実に認証が行われる。

【0037】なお、本発明は、クライアントとサーバとを中継するプロキシサーバが三台以上ある場合にも適用することが可能である。図5は、変形例にかかる認証システムを概略図により示している。図5において、認証システム200は、クライアント10、プロキシサーバ21、23、22、認証サーバ31、33、32とから構成されている。すなわち、クライアント10とAPサーバ40とを中継するプロキシサーバは三台あり、このプロキシサーバに対応して設けられている認証サーバも三台あることになる。なお、新たに設けられているプロキシサーバ23、認証サーバ33のハードウェア構成は概略他のプロキシサーバ、認証サーバと同様であるので、説明を省略する。

【0038】認証システム200では、認証サーバ31が、クライアント10に証明書31aを配布し、プロキシサーバ21に証明書31bを配布している。また、認証サーバ33は、プロキシサーバ21に証明書33aを配布し、プロキシサーバ23に証明書33bを配布している。そして、認証サーバ32が、プロキシサーバ23に証明書32aを配布し、プロキシサーバ22に証明書32bを配布している。

【0039】以下、本認証システム200におけるクライアント10、プロキシサーバ21、23、22にて実行される処理のフローチャートについて説明する。図



6、図7、図8は、それぞれプロキシサーバ21、プロキシサーバ23、プロキシサーバ22にて実行される処理の概略を示すフローチャートである。なお、クライアント10で実行される処理の概略は図2と同様である。

【0040】まず、ユーザがクライアント10からAPサーバ40へ接続要求を行うと(図2のステップS100)、プロキシサーバ21はクライアント10からAPサーバ40への接続要求を受信する(図6のステップS400)。そして、プロキシサーバ21は、ユーザの認証を認証サーバ31へ要求する(ステップS405)。認証サーバ31から認証結果を受信すると(ステップS410)、ユーザの認証が成功かどうかを判断する(ステップS415)。認証が失敗であれば、ユーザからの接続要求を拒否するとともに、接続要求拒否をクライアント10に通知し(ステップS420)、本フローを終了する。この場合、クライアント10では図示しないフローにて図2のフローを終了する。認証が成功であれば、プロキシサーバ21はプロキシサーバ23へAPサーバ40への接続要求を行う(ステップS425)。

【0041】プロキシサーバ23は、プロキシサーバ21からAPサーバ40への接続要求を受信すると(図7のステップS500)、プロキシサーバ21の認証を認証サーバ33へ要求する(ステップS505)。認証サーバ33からその認証結果を受信すると(ステップS510)、プロキシサーバ21の認証が成功かどうかを判断する(ステップS515)。認証が失敗であれば、APサーバ40への接続要求を拒否するとともに、接続要求拒否をプロキシサーバ21に通知し(ステップS520)、図7のフローを終了する。この場合、プロキシサーバ21では図示しないフローで接続要求拒否をクライアント10に通知し、図6のフローを終了する。認証が成功であれば、接続先にさらにプロキシサーバ22があるため、プロキシサーバ22へAPサーバ40への接続要求を行う(ステップS525)。

【0042】プロキシサーバ22は、プロキシサーバ23からAPサーバ40への接続要求を受信すると(図8のステップS600)、プロキシサーバ23の認証を認証サーバ32へ要求する(ステップS605)。認証サーバ32からその認証結果を受信すると(ステップS610)、プロキシサーバ23の認証が成功かどうかを判断する(ステップS615)。認証が失敗であれば、APサーバ40への接続要求を拒否するとともに、接続要求拒否をプロキシサーバ23に通知し(ステップS620)、図8のフローを終了する。この場合、接続要求拒否の通知は、さらにプロキシサーバ21、クライアント10の順に伝達され、図7と図6のフローは終了する。認証が成功であれば、自らが保有する認証済みの証明書32bを添付して、接続元のプロキシサーバ23にユーザの証明書を送信する(ステップS625)。

【0043】また、プロキシサーバ23は、プロキシ

サーバ22から、ユーザの証明書を要求を受信する(図7のステップS530)。そして、認証サーバ32で認証済みの証明書32bが添付されていることを確認する(ステップS535)。その上で、さらに認証済みの証明書33bを添付して、プロキシサーバ23は接続元のプロキシサーバ21にユーザの証明書を送信する(ステップS540)。プロキシサーバ21では、プロキシサーバ23から、ユーザの証明書を要求を受信する(図5のステップS430)。そして、認証サーバ33で認証済みの証明書33bが添付されていることを確認する(ステップS435)。その上で、さらに認証済みの証明書31bを添付して、プロキシサーバ23は接続元のプロキシサーバ21にユーザの証明書を送信する(ステップS440)。

【0044】クライアント10では、プロキシサーバ21から、所定時間内にユーザの証明書を要求を受信したかどうかを判断する(図2のステップS105)。プロキシサーバ21から接続要求拒否が通知されるか、所定時間内にユーザの証明書を要求を受信しなかった場合は、APサーバ40への接続要求を取り消す。ユーザの証明書を要求を受信した場合(ステップS110)、プロキシサーバ21が保有する認証済みの証明書31bを確認する(ステップS115)。また、プロキシサーバ23が保有する認証済みの証明書33bを確認する。さらに、証明書を要求元であるAPサーバ40に最も近いプロキシサーバ22に配布された証明書32bが添付されているとともに、認証サーバ32で認証済みであることを確認する(ステップS120)。その上で、クライアント10は、プロキシサーバ21にユーザの証明書31aを送信し(ステップS125)、図2のフローを終了する。

【0045】プロキシサーバ21では、クライアント10からユーザの証明書31aを受信し(図6のステップS445)、証明書31aが認証サーバ31で認証済みであることを確認する(ステップS450)。そして、プロキシサーバ21に配布された認証済みの証明書32aをさらに添付して、プロキシサーバ22にユーザの証明書31aを送信し(ステップS455)、図6のフローを終了する。プロキシサーバ23では、接続元のプロキシサーバ21からユーザの証明書31aを受信し(図7のステップS545)、認証サーバ33で認証済みの証明書33aが添付されていることを確認する(ステップS550)。そして、プロキシサーバ23に配布された認証済みの証明書33aをさらに添付して、プロキシサーバ22にユーザの証明書31aを送信し(ステップS555)、図7のフローを終了する。

【0046】プロキシサーバ22では、プロキシサーバ23からユーザの証明書31aを受信し(図8のステップS630)、プロキシサーバ23が保有する認証済みの証明書32aが添付されていることを確認する(ステップS635)。また、プロキシサーバ23が保有する

証明書33aを確認する。そして、ユーザの証明書31aも確認する(ステップS640)。その結果、プロキシサーバ22とユーザとが相互に認証できたこととなり、プロキシサーバ22はAPサーバ40へ接続要求を送信する(ステップS645)。すると、プロキシサーバ21、22、23を介してクライアント10とAPサーバ40との接続を確立させることが可能である。

【0047】このように、クライアントとサーバを中継するプロキシサーバが三台ある本認証システム200でも、すべての認証サーバにユーザを登録する必要がなく、各プロキシサーバにてクライアントを認証することが可能である。また、登録されたユーザの証明書を認証サーバ間で受け渡していくという特別の機能も不要である。また、中継するプロキシサーバが四台以上ある認証システムであっても、プロキシサーバ間に介在するプロキシサーバ23と同様の処理を行うことにより、上述の認証を行うことが可能となる。

【0048】

【発明の効果】以上説明したように、本発明は、登録されたユーザの証明書を認証サーバ間で受け渡す必要なく、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能な認証システムを提供することができる。また、請求項2にかかる発明によれば、サーバに最も近いプロキシサーバにて、クライアントを使用するユーザの認証を行うことが可能となる。さらに、請求項3にかかる発明によれば、プロキシサーバは、他のプロキシサーバが保有する認証済みの証明書も確認することができるので、より確実に認証を行うことが可能となる。

【0049】さらに、請求項4にかかる発明によれば、クライアントはプロキシサーバが保有する認証済みの証明書を確認することができるので、より確実に認証を行うことが可能となる。さらに、請求項5にかかる発明によれば、本システムの利用価値をより高めることができ

る。さらに、請求項6にかかる発明によれば、登録されたユーザの証明書を認証サーバ間で受け渡す必要なく、各プロキシサーバにてクライアントを使用するユーザの認証を行うことが可能な認証方法を提供することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態にかかる認証システムを示す概略図である。

【図2】クライアントにて実行される処理の概略を示すフローチャートである。

【図3】クライアントとプロキシサーバを中継するプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図4】サーバに最も近いプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図5】変形例にかかる認証システムを示す概略図である。

【図6】クライアントとプロキシサーバを中継するプロキシサーバにて実行される処理の概略を示すフローチャートである。

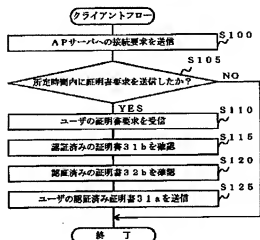
【図7】プロキシサーバどうしを中継するプロキシサーバにて実行される処理の概略を示すフローチャートである。

【図8】サーバに最も近いプロキシサーバにて実行される処理の概略を示すフローチャートである。

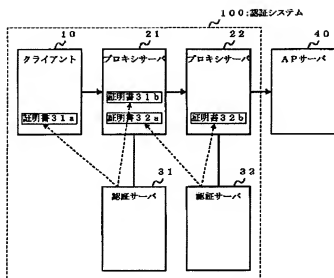
【符号の説明】

10 クライアント  
100、200 認証システム  
21、22、23 プロキシサーバ  
31、32、33 認証サーバ  
31a、31b、32a、32b、33a、33b 証明書  
40 APサーバ

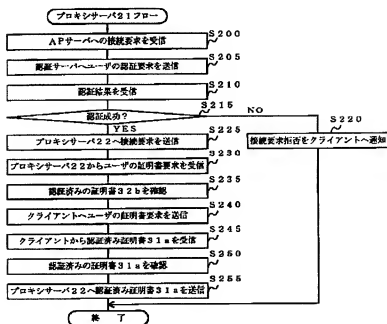
【図2】



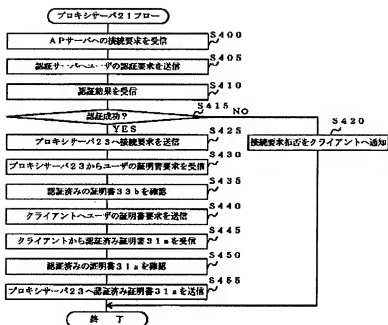
【図1】



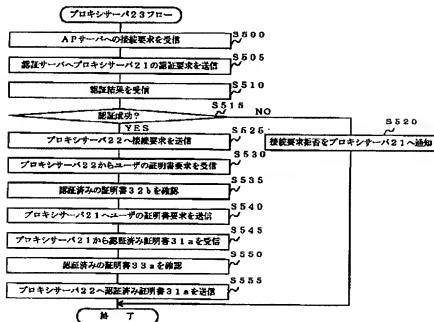
【図3】



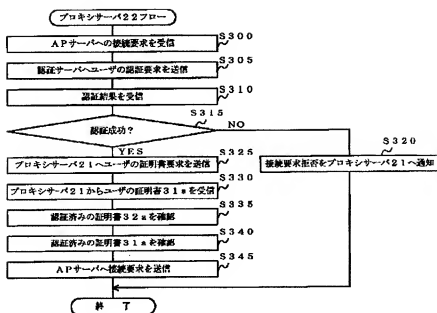
【図 6】



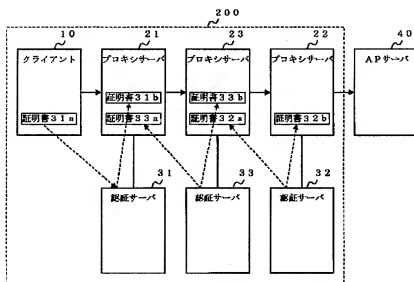
【図 7】



【図4】



【図5】



【図 8】

